International Journal of Science Engineering and Advance Technology, IJSEAT , Vol.3, Issue 10
ISSN 2321-6905
October 2015

International Journal of Science Engineering and Advance Technology

Legacy Authentication Methods Preventing Key logging Attacks

1M.Vamsi Krishna, 2 K. Nagababu
1, 2Dept. of CSE, Chaitanya Institute of Science & Technology, Kakinada, AP, India

ABSTRACT:

The objective is not protected the authentication process against the shoulder surfing attacker who be able to see or cooperation at the same time both devices over the shoulder, but quite to make it hard forthe opponent to open the attack. We show how visualization can improve not only safety but also usability by proposing two visual authentication protocols: one for password-based authentication, and the other for one-time-password. During thorough study, we show that our protocols are impervious to many of the challenging attacks appropriate to other protocols in the literature. Additionally, using an wide-ranging case study on a prototype of our protocols, we underline the potential of our protocols in real-world consumption addressing users shortcomings and limitations.

KEYWORDS: Authentication, Smartphone, Malicious code, Keylogger

I. INTRODUCTION:

The propose of secure authentication protocols is fairly demanding, bearing in mind that various kinds of root k its reside in PCs (Personal Computers) to watch user's behaviour and to make PCs untrusted devices. Involving human in authentication protocols, while talented, is not trouble-free since of their partial potential of computation and memorization. To mitigate the key logger attack, near or onscreen keyboards with slapdash keyboard arrangements are extensively used in practice. Both systems, by reorganizing alphabets erratically on the buttons, can disturb simple key loggers. Regrettably, the key logger, which has run over the entire PC, can effortlessly capture every event and read the video buffer to fashion a mapping between the clicks and the new alphabet. We show up the probable of our approach for real-world deployment: we were able to reach a high level of usability while satisfying stringent security requirements.

II. RELATED WORK:

Strongly associated work is "Seeing-is-Believing"(SiB) which uses visual channels of2D barcodes to oppose the man-in-the-middle attack in device pairing. Although we use similar tools by using the 2Dbarcodes for information representation, and the visual channel for communicating this information, our protocols are additional new generic than those proposed. Our protocols are tailored to the problem settings in hand, e-banking, with a different trust and attack model than that used in which results into different guarantees as explained earlier in this paper.

III. LITERATURE SURVEY:

THE AUTHOR, MoniNaor**(ET .AL), AIM IN [1],**this paper brings in visual authentication and visual identification methods, which are authentication and identification methods for human users based on visual cryptography. These methods are very usual and easy to use, and can be put into practice using very common \low tech" technology. The methods we propose are well-organized in the sense that a solitary clearness can be used for some authentications or for several identifications. The visual authentication methodswe proposearenotincompletetoauthenticatin gtextualmessages,and can be used to validate any image. A significant input of this paper is the forewords of a framework for establishing the security of protocols in which humans take a lively part. We rigorously prove the security of our schemes using this framework.

THE AUTHOR, XuewuGuo**(ET .AL) AIM IN [2],** Draw-A-Secret (DAS) is an archetypal carrying out based on the user drawing on a grid canvas. At present, too many constrictions product in diminution in user understanding and avert its reputation. A novel graphical password strategy Yet Another Graphical Password (YAGP) motivated by DAS is proposed in this paper. The proposal has the advantages of free drawing positions, strong shoulder surfing resistance and large password space. Experiments show the efficacy of YAGP.Alphanumeric passwords are

commonly used in computer and network authentication to protect user's privacy. Untilnow, it is well branded that long, text based passwords are tough for people to have off pat, while shorter ones are inclined to attack.

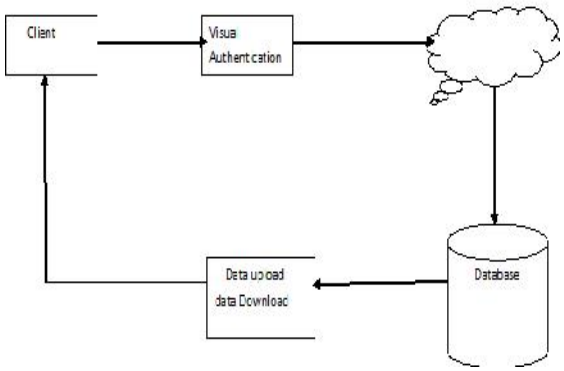
IV. PROBLEM DEFINITION:

Connecting human in authentication protocols, while talented, is not easy since of their incomplete ability of calculation and memorization. Consequently, relying on users to improve security of necessity degrades the usability. On the other hand, calming assumptions and exact security design to get better the user knowledge can show the way to protection breaks that can hurt the users' trust. It is non Security for Stored data.The intend of secure authentication protocols is rather demanding, bearing in mind that assorted kinds of root kits reside in PCs (Personal Computers) to observe user's behaviour and to make PCs untrusted devices.

V. PROPOSED APPROACH:KKKK

Witha prevalent case study on a prototype of our protocols, we underscore the credible of our come near for real-world deployment: we were endowed to comprehend a high level of usability while rewarding rigorous security requirements. It holds up sound Image security and usability and emerges to fit well with some no-nonsense applications for on the road to mending online safety.We confirm how cautious trance design can look up not only the security but also the usability of authentication. To that end, we recommend two visual authentication protocols: one is a one-time-password protocol, and the other is a password-based authentication protocol. Inexact theory test, we prove that our protocols are resistant to a lot of the demanding authentication attacks appropriate in the literature.

VI. SYSTEM ARCHITECTURE:



VII. PROPOSED METHODOLOGY:

ENCRYPTION: An encryption algorithm which takes a key kand a message M from set M and outputs a ciphertext C in the set C.

DECRYPTION:A decryption algorithm which takes a ciphertext C in C and a key k, and outputs a plaintext M in the set M.

SIGNATURE: A signature generation algorithm which takes a private key SK and a message M from the set M, andoutputs a signature.

VERIFICATION: A signature verification algorithm which takes a public key PK and a signed message, and returns valid or invalid.

QREncryption: A QR encoding algorithm which takes a string S in S and outputs a QR code.
QRDecryption: A QR decoding algorithm which takes a QR code and returns a string S in S.

AUTHENTICATION ALGORITHM

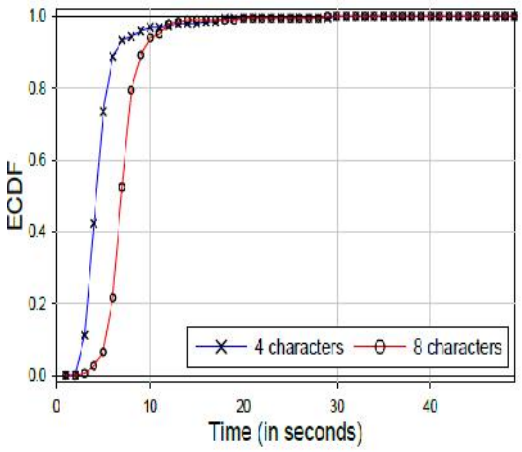
STEP1: The user connects to the server and sends her ID.

STEP2: The server checks the ID to recover the client's public key from the database. The server then picks a new arbitrary string OTP and scrambles it with the general public key to get EOTP.
STEP3: A QR code QREOTP is displayed prompting the user to type in the string.

STEP4: The client interprets the QR code with EOTP in light of the fact that the arbitrary string is encoded with client's public key, the client can read the OTP string and sort in the OTP in the terminal with a physical console.

STEP5: The server checks the outcome and on the off chance that it coordinates what the server has sent before, the client is verified. Something else, the client is denied.

VIII. RESULTS:



The usualsuccess rate was 98:0% with 4-character passwords and 92:5%for 8-character passwords. An experiential CDF of the timemeasurements is shown. We originate that the mean,min, max and median (in seconds) were 4:25, 2, 29, and 4when using 4-character passwords and 6:74, 2, 28, and 6 whenusing 8 characters.

IX. ENHANCEMENT:

To Improve Proposed methodology execution ring imprint give lack of clarity of client. Which infers that the verifier understands that the client is a person from a ring, yet he doesn't know absolutely who the client is.

X. CONCLUSION:

Wechart to look into the proposal of other protocolwith more severepresentationneedsby means of the sametools make available in this work. In addition, we will learn methodsfor getting better the security and user knowledge by means ofvisualization in other contexts, but not incomplete to authenticationsuch as visual decryption and visual signature confirmation.At last, treatment on user studies that will advantage from abroaduse and receipt of our protocols would be asimilar future work to consider as well.

XI. FUTURE WORK:

At last, investigating client contemplates that will advantage by a wide course of action and confirmation of our customs would be a parallel future work to consider too.

XII. REFERENCES:

[1] —. Google authenticator. http://code.google.com/p/ google-authenticator/.
[2] —. Rsasecurid. http://www.emc.com/security/rsa-securid.htm.
[3] Cronto. http://www.cronto.com/.
[4] —. BS ISO/IEC 18004:2006. information technology. automatic identification and data capture techniques. ISO/IEC, 2006.
[5] —. ZXing. http://code.google.com/p/zxing/, 2011.
[6] D. Boneh and X. Boyen. Short signatures without random oracles. In Proc. of EUROCRYPT, pages 56–73, 2004.
[7] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In Security and Privacy (SP), 2012 IEEE Symposium on, pages 553–567. IEEE, 2012.
[8] J. Brown. Zbar bar code reader, zbar android sdk 0.2. http://zbar. sourceforge.net/, April 2012.
[9] C.-H. O. Chen, C.-W. Chen, C. Kuo, Y.-H. Lai, J. M. McCune, A. Studer, A. Perrig, B.-Y. Yang, and T.-C. Wu. Gangs: gather, authenticate 'n group securely. In J. J. Garcia-Luna-Aceves, R. Sivakumar, and P. Steenkiste, editors, MOBICOM, pages 92–103. ACM, 2008.
[10] S. Chiasson, P. van Oorschot, and R. Biddle. Graphical password authentication using cued click points. In Proc. of ESORICS, 2008.
[11] D. Crockford. The application/json media type for javascript object notation (json). http://www.ietf.org/rfc/rfc4627.txt?number=4627, July 2006.
[12] D. Davis, F. Monrose, and M. Reiter. On user choice in graphical password schemes. In Proc. of USENIX Security, 2004.
[13] N. Doraswamy and D. Harkins. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall, 2003.
[14] M. Farb, M. Burman, G. Chandok, J. McCune, and A. Perrig. Safeslinger: An easy-to-use and secure approach for human trust establishment. Technical report, CMU, 2011.
[15] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu. Yagp: Yet another graphical password strategy. In Proc. of ACM ACSAC, pages 121–129, 2008.

Mr.M VAMSI KRISHNA received the M Tech CS in Allahabad University, M.Tech (AI & R) degree in Andhra University, and Ph.D from Centurion University, Odisha. Currently he is working as Professor & HOD in Department of Computer Science and Engineering. He has 15 years of experience in teaching. His research interests

include Artificial intelligence, computer networks, image processing.

Mr.K.Nagababu is a student of Chaitanya Institute of Science & Technology, Kakinada. Presently he is pursuing his M.Tech [Software Engineering] from this college and he received his B.Tech from Sri Sai Aditya institute of Science & Technology, affiliated to JNT University, Kakinada in the year 2009. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.